UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,745	06/19/2000	Carl J. Kraenzel	LOT9 2000 0011 US1	3997

7590 07/09/2003

Stephen T. Keohane, Esq.
Lotus Development Corporation
55 Cambridge Parkway
Cambridge, MA 02142

EXAMINER
WINTERS, MAREISHA N

ART UNIT	PAPER NUMBER
2153	9

DATE MAILED: 07/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/596,745	KRAENZEL ET AL.	
	Examiner	Art Unit	
	Mareisha N. Winters	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 May 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed on May 6, 2003. Claims 1, 7, 12, and 17-19 have been amended.

2. Claims 1-19 remain pending in the application.

Drawings

3. The corrected or substitute drawings were received on May 6, 2003. These drawings are accepted.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,473,800 to Jerger et al. (hereinafter "Jerger") in view of U.S. Patent No. 5,974,549 to Golan (hereinafter "Golan").

In considering **claim 1**, Jerger discloses a system for a web based trust model governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform, comprising:

a connection protocol connecting a user client to a server site (column 1, lines 41-44);

download utilities responsive to said connection protocol for downloading said services and programs from said server site to said user client (column 3, lines 15-16); and

trust assignment user interface dialogs responsive to said connection protocol for advising said user of risks taken when accepting executable download from said server site (see Fig. 5B and column 2, lines 27-31 and 36-38 and column 19, lines 66-67 and column 20, lines 1-6).

Although the system disclosed by Jerger shows substantial features of the claimed invention, as discussed above, it fails to disclose:

downloading said services and programs from said server site to *separate and non-conflicting execution spaces at* said user client; nor

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Golan.

In an analogous art, Golan discloses a system for securing untrusted and/or unknown software downloaded from an external source comprising:

downloading said services and programs from said server site to separate and non-conflicting execution spaces at said user client (column 2, lines 20-25 and column 6, lines 1-5); and

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs (column 7, lines 1-9). Given the teaching of Golan, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Jerger by employing the well known features of (1)

non-conflicting, wholly separate execution spaces, and (2) centrally managed security policy, such as disclosed by Golan, in order to:

(1) Prevent the downloadable from accessing and modifying other areas of the system to which they do not have permission; and

(2) Limit the authority of the end user who may not have advanced knowledge of security issues.

In considering **claim 2**, Jerger discloses said connection protocol selectively being HTTP or HTTPS (see Fig. 4B, "433" and column 18, lines 8-10 and column 17, lines 61-66).

In considering **claim 3**, Jerger discloses the system further comprising:

a processor for establishing security context (see column 14, lines 52-54), said processor including

a stage 1 processor for determining from said user if said server site is to be trusted (see column 14, lines 54-57 and 64-67); and

a stage 2 processor for establishing whether or not the identity of said web site is confirmed and determining from said user if processing should continue to include installation of programs on said client (see column 20, lines 2-11).

In considering **claim 4**, Jerger discloses the system further comprising:

a client download page (see column 3, lines 29-32);

a download control element in said download page (see column 3, lines 29-32);

said processor being activated upon activation of said download control element within said download page initiating a download process first to establish a security context and then to download program executable files (see column 3, lines 32-37).

In considering **claim 5**, Jerger discloses the system further comprising:

said download utilities being responsive to an SSL connection to said server for activating said dialog to advise said user that said server site has been verified as being what it represents itself to be and to query said user whether code is to be downloaded from said server site to said client (see column 18, lines 13-16 and Fig. 4B, "433" and column 20, lines 2-11).

In considering **claim 6**, Jerger discloses said code being custom code (see Fig. 5B).

In considering **claim 7**, Jerger discloses said download utilities being responsive to a connection from said client to said server being other than SSL for activating said dialog to advise said user that said server site has not been verified as being what it represents itself to be and to query said user whether code is to be downloaded from said server site to said client (see column 22, lines 13-14 and lines59-60).

In considering **claim 8**, Jerger discloses said code being custom code (see Fig. 5B).

In considering **claim 9**, Jerger discloses the system further comprising:

said download utilities being responsive to user acceptance of download from said server site of executable code for downloading said executable code to said client (see column 18, lines 27-28 and Fig. 5B); and

a trace utility for identifying originators of downloaded code (see column 22, lines 9-13).

In considering **claim 10**, Jerger discloses said trace utility selectively identifying originators of signed agents through electronic signature, of custom code traceable to code vendor through web site relationship, or custom code directly created by said web site (see column 22, lines 9-13).

In considering **claim 11**, Jerger discloses the system further comprising:

a first trust model for establishing level of traceable accountability for a subscription at download time over a secure connection protocol (see column 23, lines 33-37 and 47-50);

a second trust model for establishing a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said subscription over a connection protocol not verified as secure (see column 24, lines 35-42); and

said dialogs being responsive to said trust models (see Fig. 5B, "510").

In considering **claim 12**, Jerger discloses a method for governing delivery of services and programs from a workflow, enterprise and mail enabled application server and platform according to a web based trust model, comprising the steps of:

establishing a connection protocol between a client and a web site (see column 1, lines 41-44);

responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);

advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-38 and Fig. 5B); and

responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20, lines 5-6; Note that if the user selects "yes" the operation, i.e. downloading services and programs, is to be performed.).

Although the system disclosed by Jerger shows substantial features of the claimed invention, as discussed above, it fails to disclose:

downloading said services and programs from said server site to *separate and non-conflicting execution spaces at* said user client; nor

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Golan.

In an analogous art, Golan discloses a system for securing untrusted and/or unknown software downloaded from an external source comprising:

downloading said services and programs from said server site to separate and non-conflicting execution spaces at said user client (column 2, lines 20-25 and column 6, lines 1-5); and

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs (column 7, lines 1-9). Given the teaching of Golan, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Jerger by employing the well known features of (1) non-conflicting, wholly separate execution spaces, and (2) centrally managed security policy, such as disclosed by Golan, for the reasons given above with respect to claim 1.

In considering **claim 13**, Jerger discloses the method further comprising the steps of:

displaying a download control element in a client download page (see column 3, lines 29-32);

responsive to user selection of said download control element or upon schedule, initiating a download process first to establish a security context and then to download program executable files from said server (see column 3, lines 32-37).

In considering **claim 14**, Jerger discloses the method further comprising the step of responsive to user acceptance of download from said server site of executable code, downloading said executable code to said client (see column 18, lines 27-28 and Fig. 5B).

In considering **claim 15**, Jerger discloses the method further comprising the step of identifying originators of downloaded code (see column 22, lines 9-13).

In considering **claim 16**, Jerger discloses the method further comprising the step of selectively identifying originators of signed agents through electronic signature, of custom code traceable to code vendor through web site relationship, or custom code directly created by said web site (see column 22, lines 9-13).

In considering **claim 17**, Jerger discloses the method further comprising the steps of:

establishing a first trust model specifying a level of traceable accountability for a subscription at download time over a secure connection protocol (see column 23, lines 33-37 and 47-50);

establishing a second trust model for specifying a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said subscription over a connection protocol not verified as secure (see column 24, lines 35-42); and

said dialogs being responsive to said trust models (see Fig. 5B, "510").

In considering **claim 18**, Jerger discloses a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, said method steps comprising:

establishing a connection protocol between a client and a web site (see column 1, lines 41-44);

responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);

advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-68 and Fig. 5B); and

responsive to user acceptance of said risks and I accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20, lines 5-6; Note that if the user selects "yes" the operation, i.e. downloading services and programs, is to be performed.).

Although the system disclosed by Jerger shows substantial features of the claimed invention, as discussed above, it fails to disclose:

downloading said services and programs from said server site to *separate and non-conflicting execution spaces at* said user client; nor

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs. Nonetheless, these features are

well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Golan.

In an analogous art, Golan discloses a system for securing untrusted and/or unknown software downloaded from an external source comprising:

downloading said services and programs from said server site to separate and non-conflicting execution spaces at said user client (column 2, lines 20-25 and column 6, lines 1-5); and

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs (column 7, lines 1-9). Given the teaching of Golan, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Jerger by employing the well known features of (1) non-conflicting, wholly separate execution spaces, and (2) centrally managed security policy, such as disclosed by Golan, for the reasons given above with respect to claim 1.

In considering **claim 19**, Jerger discloses a computer program product configured to be operable to govern delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, according to the steps of:

establishing a connection protocol between a client and a web site (see column 1, lines 41-44);

responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site (see column 14, lines 49-52 and column 16, lines 41-50);

advising a user at said client of said trust level assignable with respect to said risks to said web site (see column 2, lines 27-31 and 36-38 and Fig. 5B); and

responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to said user client (see column 20, lines 5-6; Note that if the user selects "yes" the operation, i.e. downloading services and programs, is to be performed.).

Although the system disclosed by Jerger shows substantial features of the claimed invention, as discussed above, it fails to disclose:

downloading said services and programs from said server site to *separate and non-conflicting execution spaces at* said user client; nor

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs. Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Jerger, as evidenced by Golan.

In an analogous art, Golan discloses a system for securing untrusted and/or unknown software downloaded from an external source comprising:

downloading said services and programs from said server site to separate and non-conflicting execution spaces at said user client (column 2, lines 20-25 and column 6, lines 1-5); and

said server site responsive to said user accepting said server site as trusted for centrally administering security policies for said services and programs (column 7, lines 1-9). Given the teaching of Golan, a person having ordinary skill in the art would have readily recognized the

desirability and advantages of modifying Jerger by employing the well known features of (1) non-conflicting, wholly separate execution spaces, and (2) centrally managed security policy, such as disclosed by Golan, for the reasons given above with respect to claim 1.

Response to Arguments

6. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,233,341 to Riggins

U.S. Patent No. 6,301,661 to Shambroom

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mareisha N. Winters whose telephone number is (703) 305-7838. The examiner can normally be reached on Monday-Friday, 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton B. Burgess can be reached on (703) 305-4792. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for official communications, (703) 746-7240 for non-official communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Mareisha N. Winters
Patent Examiner
Art Unit 2153
July 1, 2003

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100